



EMACS SECURITY REQUEST POLICY AND PROCEDURE MANUAL



EMACS Security Request Policy and Procedure

POLICY	2
EMACS Access	2
Audit of User Security	3
Procedures	3
Definitions	3
Roles	5



EMACS Security Request Policy and Procedure

POLICY

This policy establishes a process developed in conjunction with and as an extension of County Policy 09-06, 'Computer System Data Security' as it relates to the security of the data housed in the Employee Management and Compensation System (EMACS).

EMACS is an Oracle PeopleSoft Human Capital Management (HCM) application that integrates business processes of Human Resources (HR) and Auditor-Controller/Treasurer/Tax Collector (ATC) to manage employee's job, pay, and benefits for the County, County Fire, Special Districts, and SBCERA.

Due to the sensitive nature of the data contained within EMACS, all employees acknowledge their responsibility in accessing this information every time they sign into and use EMACS. The following is language that appears on the EMACS sign in screen for every employee each time they sign in:

******* WARNING *******

SELF-SERVICE USERS: The use of this system does not waive your privacy rights regarding your personal information.

NON SELF-SERVICE USERS: Not for personal use - all records are subject to review. There should be no expectation of personal privacy related to the use of this system.

Data contained in this system is confidential and protected by state and federal law. Every employee who uses the EMACS system must recognize his or her responsibility for the security of the system and the information contained therein. Access to this system is recorded. Attempts to retrieve or share EMACS information not necessary to perform your job duties are strictly prohibited. Unauthorized access may result in disciplinary action, up to and including termination and prosecution under applicable laws.

Authorized Use

Any unauthorized use of EMACS constitutes failure to adhere to County Policy and/or procedure. In accordance with Personnel Rule 10 – Disciplinary Actions, an employee who demonstrates willful or negligent disobedience of any law, ordinance, Memorandum of Understanding, County or Department rule, regulation, policy or procedure may be subject to disciplinary action.

EMACS Access

Access will be restricted to those who need it and in accordance with their scope of their duties. For example, if Departments have only one Payroll Specialist, that person would only need access to efficiently process payroll for their respective department. If Departments have employees in several classification who perform different functions, access will be limited to their required duties.



EMACS Security Request Policy and Procedure

Employees having access to personnel and payroll data must only use this information for job-related purposes and not for personal use for themselves or others. Sensitive data may be shared only with employees within their own department who need the information to perform their job responsibilities. All data users are acknowledging their responsibility to maintain the integrity of the data accessed every time they log into EMACS.

Audit of User Security

User security shall be reviewed/audited in the following instances:

- Position changes – when a position is changed, transferred, activated, or deactivated EMACS-Dev shall delete the security attached to that position, when notified via a revised EMACS Security Request Form.
- Periodic basis - EMACS-Dev, in conjunction with the Employee Relations division of Human Resources, will conduct an audit of all departmental and Countywide access on an annual basis. Based on the results of the audit, individual access will be adjusted based on current job duties. The audit shall be conducted in March of every year and the results of such audit shall be reported to the Director of Human Resources.

Procedures

It is the department's responsibility to request security access for employees whose job functions require the use of the EMACS system. Access is position based, not employee ID based. Access for each position can be added, revised, or deleted. Departmental access can be granted by individual department ID's or by providing a range of department ID's.

Definitions

Authorized User - individuals who access confidential/payroll/personnel data in order to perform their assigned duties or to fulfill their role to the County.

EMACS - an Oracle PeopleSoft HRMS application that houses employee and business process data to manage employees, their pay, and benefits for the County, County Fire, Special Districts and SBCERA.

Official Personnel File (OPF) - a County of San Bernardino document repository governed by the Information Services Department (ISD), which contains employee Personnel Files.

Role - the term role as used in the context of this policy shall mean the function assumed by or assigned to person or thing in a particular situation.



EMACS Security Request Policy and Procedure

Responsibilities

Department Contact/Appointing Authority responsibilities include, but are not limited to:

- Determine and establish an authorized user.
- Update an authorized user who has terminated employment with the County
- Update an authorized user who transfers to another department or a division within the department
- Update an authorized user who promotes or demotes
- Update an authorized user who may be absent over an extended period of time
- Update an authorized user's access when it may jeopardize an investigation or constitute negligence on the part of the County
- Update an authorized user who is a threat to the workplace
- Update an authorized user's access because their scope of duties have changed requiring them to no longer require access to EMACS, in part or in whole.

EMACS-Dev responsibilities include, but are not limited to:

- Develop and maintain Standard Practices to implement this Policy.
- Identify and resolve security problems associated with the use of EMACS
- Provide guidance to HR, Central Payroll, and Departmental users in the handling of EMACS security problems.
- Review and appropriately assign/update EMACS Security to authorized users.

Human Resource Officer (HRO) / Employee Relations Chief responsibilities include, but are not limited to:

- Review access request to determine if requested access is necessary for job functions
- Grant access or return form to requestor without access

For Human Resources Department, The Employee Relations Chief reviews and approves the request in place of the HRO signature



EMACS Security Request Policy and Procedure

Roles

The following is a summary of the most frequently utilized roles and a brief description of their functions including the most common page access provided in EMACS.

Role	Access Description
Security	
Payroll Specialist Profile	Employees primarily assigned to a payroll/personnel section, requiring access to Job Data, Position Data, Emergency Contact, Benefits Data, Leave Accrual panels, Employment Data, Job Data, Absence History, WPE, Step History, Personal Data, Payroll Data, and Paycheck Data.
Manager/Supervisor	Employees in a supervisory or management level position requiring access to Job Data, Position Data, WPE, Personal Data, Emergency Contact, Online PR, Absence History, and Leave Accrual panels.
Budget Preparation	Employees assigned to a fiscal section performing budget preparation requiring access to Benefits, Pay Rate and Position Data pages.
Phone Coordinator	Limited access to update an employee's business phone number information which is then sent to ISD to update Countyline
Modified Duty Representative (Departmental Modified Duty Coordinator)	Access to Benefits Data, Leave Accrual Page, Payroll Data, Paycheck Data, Position Data, and Absence Summary Page.
Modified Duty Representative (Risk Management)	Access to track and enter modified duty information as well as run MD Reports.
eTime	
DTA Department Time Administrator	Provides ability for department designee to coordinate, monitor, review, and correct all employee timesheets and payroll processing exceptions for their department
DSA Department Security Administrator	Provides ability for department designee to maintain the time approval hierarchy within their respective department. Assign Manager/Approver for each employee in his or her department.
DTR Department Time Reporter	Provides ability for department designee to enter and submit time on behalf of employees who are not able to electronically access EMACS
RO Read Only Access	Access limited to view employees' timesheets



EMACS Security Request Policy and Procedure

Online PR	
Requestor	Access limited to Online Personnel Requisition, Certification List Request - (for workflow purposes only - limits the access to which positions a requestor can requests for)
Approver Dept. Approver Admin Approver Agency Approver CAO Approver	Access limited to Online Personnel Requisition (for workflow purposes only – limits the access to which positions an approver can approve) There are four levels of approval authorization: Department, Administrative, Agency, & CAO.
Hire Processor <i>NEOGOV</i>	Access limited to Online Personnel Requisition, Hire Notification (for workflow purposes only - notifies the designated "hire processor" for that department an employee has been hired)

Security Access Request for EMACS Form

The Security Access Request (SAR) for EMACS form provides access to EMACS and/or Online Personnel Requisition (PR) Access in NEOGOV. The SAR for EMACS must be reviewed and approved by your department's Human Resources Officer (HRO) prior to access being granted.

